IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA,	)	
	)	
v.	)	Case No. 1:23CR65-CMH
	)	
JAMES MEEK.	)	

MOTION TO SUPPRESS CONTENTS OF DEFENDANT'S INTERNET ACCOUNTS

James Gordon Meek, through counsel, and pursuant to the Fourth Amendment to the United States Constitution, moves this Court for an order suppressing the entire contents of Mr. Meek's Internet accounts seized pursuant to a "preservation letter" as a fruit of its unlawful seizure in violation of the Fourth Amendment. The following accounts were seized in violation of the Fourth Amendment:

Provider	Account	Date of Preservation Letter	Date of Search Warrant
Google	[redacted]	March 10, 2021	No warrant provided in discovery.[1]
Dropbox	Account associated with [redacted]	September 9, 2021	November 10, 2021.[2]
Google	[redacted]	January 18, 2022	No warrant provided in discovery. Grand jury subpoena was served on Google and

[1] As set forth in the motions to compel, the government has not fully complied with its discovery obligations, so it is possible that this account was searched under an undisclosed warrant. Nevertheless, as discussed below, there was an unlawful warrantless seizure of this and other accounts as a result of the government's preservation letter, regardless of whether the government ultimately obtained a warrant for the account. Google provided results in response to an 18 U.S.C. § 2703(d) order.

[2] On November 22, 2021, Dropbox allegedly responded that given the absence of a preservation letter within 90 days, the account content was not preserved. However, given the incompleteness of discovery, we include this account here in case the government later discusses that contents of the account were seized.

			Google provided results.
Dropbox	Account associated with [redacted]	January 19, 2022	No warrant provided in discovery. Grand jury subpoena served on March 17, 2022, resulting in information obtained by government on March 23, 2022.
Apple	Apple internet accounts associated with the email [redacted]	August 26, 2022. Extension request sent on or about November 21, 2022.	November 14, 2022.
Apple	Apple iCloud account associated with the email address [redacted]	October 4, 2022	November 14, 2022
Snapchat	Account associated with the username [redacted]	October 4, 2022	November 14, 2022
Snapchat	Accounts associated with the username [redacted] and [redacted]	November 15, 2022	None provided in discovery.
Google	Email account [redacted]	November 21, 2022	No warrant provided in discovery.
Kik	JHuuul4	November 9, 2022	No warrant provided in discovery.
Google	Jhuuul4@gmail.com	November 9, 2022	No warrant provided in discovery.
Twitter	Jlugne	November 21, 2022	No warrant provided in discovery.
Microsoft	Skype user account [redacted] or [redacted]	September 9, 2021. Extension request submitted November 30, 2021.	No warrant provided in discovery.
Meta	Instagram accounts [redacted]	September 14, 2022.	No warrant provided in discovery.

INTRODUCTION

Defendant's private messages in his personal Internet account were seized at the government's direction under the claimed authority of a federal statute, 18 U.S.C. § 2703(f) (hereinafter, "the preservation statute"). The preservation statute provides that, "upon the request

of a governmental entity," Internet providers "shall . . . retain[]" files in a user's account "for a period of 90 days," renewable for another 90 days. *Id.*

The government believes that the preservation statute allows the government to order copies made of the contents of any person's Internet account, and to have those contents held for the government for up to 180 days, without any cause whatsoever. Based on this understanding, the foregoing providers, acting as the government's agent, seized defendant's private contents and held them on the government's behalf as specified above.

This long-term, government-directed, warrantless seizure of Mr. Meeks personal messages and other internet private documents cannot be reconciled with the Fourth Amendment. Instead of preservation occurring "pending the issuance of a court order," 18 U.S.C. § 2703(f)(1), as the Fourth Amendment and the plain text of the statute require, the government used the preservation statute to gain control of Mr. Meek's accounts just in case probable cause eventually developed. The government ordered the seizure of the accounts without probable cause or even reasonable suspicion.

The Fourth Amendment protects the private e-mails and private messages in a password-protected online account. A government-directed copying and setting aside of a person's private account is a Fourth Amendment seizure. Such a warrantless seizure is permitted under the Fourth Amendment only in very limited circumstances, generally based on probable cause and permitted only for a brief period of time. Because the warrantless seizures in this case occurred without any justification and for an extended period, the fruits of those seizures—the contents of the preserved accounts—must be suppressed.

STATUTORY AND FACTUAL BACKGROUND

The Stored Communications Act, 18 U.S.C. §§ 2701-11, is a federal statute that regulates government access to the private records of Internet users. Internet providers such as Google, Apple, and Snapchat hold their users' records on their computer network servers. When criminal investigators seek copies of records from the accounts of proposed suspects, investigators obtain the records directly from the Internet providers. The Stored Communications Act establishes the responsibilities and duties of both the government and Internet providers when the government seeks user information. *See generally* 2 WAYNE LAFAVE, ET AL., CRIMINAL PROCEDURE § 4.8 (4th ed. 2015) (presenting overview of the statute).

This case involves the Stored Communications Act's preservation statute found at 18 U.S.C. § 2703(f). The statute provides:

> (f) Requirement To Preserve Evidence.
> (1) In general.— A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.
> (2) Period of retention.— Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

The preservation statute was enacted to ensure government access to user records that might otherwise be deleted before the government obtained legal process. Because obtaining legal process can be time-consuming, the preservation statute "permits the government to direct providers to 'freeze" stored records and communications" of suspects pending the issuance of a warrant or other court order. U.S. DEP'T OF JUST., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 139 (2009).

The key question is when the preservation statute can be used. The government and major Internet providers interpret 18 U.S.C. § 2703(f) to permit unlimited preservation of

Internet accounts. *See* Orin S. Kerr, *The Fourth Amendment Limits of Internet Content Preservation*, 65 St. Louis U. L.J. 753, 766-78 (2021) (summarizing government and provider practices) (hereinafter Kerr, *Internet Content Preservation*). As the government interprets the law, the statute allows any government agent, at any time, to order any provider to make and set aside a copy of every file, of any Internet account, without any suspicion whatsoever. *See id.* The government calls this process "preservation," but it is really just suspicionless seizing. Acting on the government's instruction, and as the government's agents, Internet providers make complete copies of target accounts and save them exclusively for later government use. *See id.* at 784-85.

Based on the belief that the § 2703(f) permits such mass-scale seizures without cause, the federal government and state governments order the preservation of hundreds of thousands of Internet accounts every year. *See id.* at 767-69. This dragnet surveillance practice has gone unchallenged for many years. *See id.* at 755-56. Major Internet providers and the government work together to make this process both automatic and largely secret. *See id.* at 775-78. When a government agent makes a § 2703(f) request, providers will copy and preserve the account contents without question. *See id.* at 772. In the ordinary case, this process is hidden from users. Internet providers do not tell their customers that preservation occurred. And the government ordinarily does not disclose preservation. *See id.* at 775-78.

This case presents a rare constitutional challenge to § 2703(f) preservation because it is a rare case when the fact of preservation was disclosed. On the dates set forth above, the government submitted a § 2703(f) request to the Providers directing the preservation of Mr. Meek's Accounts. In response to most or all of those requests, the Providers made a copy of Mr. Meek's Accounts. The Providers then set aside the copy and held it for the government. While it is not clear how long the account data was held in some cases, in cases where the government

obtained a warrant it was held for over a month, and in some instances longer than a month. But regardless of whether the government obtained a warrant, the seizure of the account content without probable cause violated Mr. Meek's Fourth Amendment rights, and the illegally seized content should therefore be suppressed.

ARGUMENT

The warrantless preservation of Mr. Meek's Internet accounts violated his Fourth Amendment rights. The preservation was government action because it required the providers to act on the government's behalf. Preservation triggered a Fourth Amendment seizure because it eliminated Mr. Meek's exclusive control of his accounts. It was an unreasonable seizure because it was not based on probable cause or even reasonable suspicion and was not followed promptly by a warrant. Further, the Terms of Service governing the provider accounts did not eliminate Mr. Meek's Fourth Amendment rights. The contents of the account must be suppressed because they are fruits of the unconstitutional preservation and no good-faith exception can apply. The analysis below addresses each point in turn.

A. THE PRESERVATION OF MR. MEEK'S ACCOUNTS WAS FOURTH AMENDMENT STATE ACTION.

The provider's act of preserving Mr. Meek's accounts pursuant to 18 U.S.C. § 2703(f) was government-directed action regulated by the Fourth Amendment. The Fourth Amendment applies to acts of private individuals acting as "instrument[s] or agent[s]" of the Government. *Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971). A private party acts as a government agent when the government "compelled a private party to perform a search" or the private party otherwise acted pursuant to the "encouragement, endorsement, and participation" of the government. *Skinner v. Railway Labor Executives' Assn.*, 489 U.S. 602, 613–614 (1989).

That test is satisfied here. Section 2703(f) states that "upon the request of a governmental entity," the provider "*shall take all necessary steps* to preserve records and other evidence" in its possession, and that the records "*shall be retained* for a period of 90 days, which *shall be extended* for an additional 90-day period upon a renewed request by the governmental entity." 18 U.S.C. § 2703(f) (emphasis added). By triggering the preservation statute, the government directed what the Providers must do. In response, the Providers fulfilled the government's wishes on the government's behalf. This mandate satisfies the test for state action. *See Skinner*, 489 U.S. at 613 (noting that "compell[ing] a private party to perform a search" makes that private party a Fourth Amendment state actor).

The preservations in this case are Fourth Amendment government action even if compliance with § 2703(f) is considered voluntary instead of a mandatory obligation. In *Commonwealth v. Gumkowki*, 167 N.E.3d 803 (Mass. 2021), a state trooper asked the cellular and Internet service provider Sprint to voluntarily disclose a suspect's cell-site location records without a warrant. Sprint agreed. The Court ruled that Sprint's voluntary disclosure constituted Fourth Amendment state action: When "law enforcement instigates the search by contacting the cell phone company to request information, there is State action. That Sprint could have refused to provide records in response to [the state trooper's] request does not change the fact that he instigated the search." *Id.* at 812.

United States v. Hardin, 539 F.3d 404 (6th Cir. 2008), confirms the point. In *Hardin*, an apartment manager entered an apartment at the request of the government to see if the defendant was present. The Sixth Circuit ruled that the apartment manager was a Fourth Amendment state actor. *Id.* at 407. This was true, the court ruled, "because the officers urged the apartment

manager to investigate and enter the apartment, and the manager, independent of his interaction with the officers, had no reason or duty to enter the apartment." *Id*.

When the Providers complied with the government's directive under the preservation statute, both the government and the Providers believed that the Providers' compliance with the government's "request" was mandatory. The statute imposes an obligation: It states what a provider "shall" do when it receives a preservation request. 18 U.S.C. § 2703(f). This is not merely "instigat[ing]" the provider's act under *Gumkowski* and *Hardin*, it is "compell[ing] a private party" to act under *Skinner*. But whether the preservation is construed as ordering or merely instigating the act of preservation, it is state action under the Fourth Amendment.

B. PRESERVATION OF MR. MEEK'S ACCOUNTS WAS A FOURTH AMENDMENT SEIZURE.

A Fourth Amendment seizure occurs "when there is some meaningful interference with an individual's possessory interests in that property." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). The classic example of a seizure is physical taking away of property. Being "dispossessed" of your property by government action causes a seizure of it. *Soldal v. Cook County*, 506 U.S. 56, 61 (1992) (towing away a mobile home).

Preservation of Mr. Meek's accounts caused a Fourth Amendment seizure because it dispossessed him of control over the information in the accounts. Internet providers "execute preservation requests by making a copy of the full contents of the relevant account and storing it separately." Kerr, *Internet Content Preservation*, at 771. Although this process is labeled 'preservation,' it reality it is "a dynamic process of entry, copying, and storage." *Id*. at 782. As Internet providers have themselves explained, this is done by performing a "data pull" of the contents of the account that take a "snapshot" of the account contents. *Id.* (quoting public

statements from Twitter and Apple). The copy is then stored outside the user's control so the user cannot alter or delete any files. *Id.* at 784-85.

The government-directed act of creating a government copy of the account, and storing it away for later government access, caused a "meaningful interference" with Mr. Meek's "possessory interests in that property" because it denied him control over his private information. *Jacobsen*, 466 U.S. at 113. "Possession" is defined as the "detention and control. . . of anything which may be the subject of property." BLACK'S LAW DICTIONARY 1047 (5th ed. 1979). Before preservation occurred, Mr. Meek had control of his account contents. He could view this content, he could alter his content, and he could delete the content as he wished.

Preservation eliminated that control. Preservation ensured that a perfect copy of the account contents was generated and detained outside his control exclusively for the government's future use. This was done for the express purpose, and with the exact effect, that Mr. Meek could no longer control the contents of his account. Preservation therefore triggered a seizure. *See United States v. Bach*, 310 F.3d 1063, 1067-68 (8th Cir. 2002) (analyzing the copying and review of stored Internet contents held by an Internet provider as a Fourth Amendment "seizure" and a "search" of the contents); *Vaugh v. Baldwin*, 950 F.2d 331, 334 (6th Cir. 1991) (noting that, in the absence of consent, the government had "no right to . . . photocopy" a person's private documents); *United States v. Loera,* 333 F. Supp. 3d 172, 185 (E.D.N.Y. 2018) ("Most courts that have addressed duplication, including digital duplication, have analyzed it as a seizure."); Fed. R. Crim. Pro. 41(e)(2)(B) (equating the seizure of electronically stored information with the copying of the information).[3]

[3] The Second Circuit expressly held that copying a file is a seizure in a panel decision that was later vacated on rehearing *en banc*; the *en banc* court did not reach the question. *See United States v. Ganias*, 755 F.3d 125, 137 (2d Cir. 2014) (holding that the Government's retention of

In the data context, of course, the government dispossesses a person of control without physically removing the data. But that makes no legal difference. Copying private files triggers a seizure because the government gains control of the data. The government's gaining control and a user's losing exclusive control causes a seizure even though the user still has access to a prior copy of the data. *See United States v. Jefferson,* 571 F. Supp. 2d 696, 703 (E.D. Va. 2008) (holding that "recording . . . information by photograph or otherwise" is a seizure, "even if the document or disc is not itself seized," because "the Fourth Amendment privacy interest extends not just to the paper on which the information is written or the disc on which it is recorded but also to the information on the paper or disc itself"). The government cannot simply take control of the contents of everyone's private Internet messages, just as long as the government does not (yet) look at the files, entirely at the government's whim. Preservation triggers copying of the account, and that copying is a Fourth Amendment seizure permitted only if it is constitutionally reasonable. *See id.*

It should be especially clear that preservation is a Fourth Amendment "seizure" given how Internet search warrants are executed under the Stored Communications Act as required by the Fourth Amendment. *See Warshak v. United States*, 631 F.3d 266, 274 (6th Cir. 2010) (holding that accessing private emails is a Fourth Amendments search that requires a warrant). When the government serves a warrant on a provider under § 2703(a), the provider will run off a copy of the account and send the copy to the government for its review. The provider conducts the initial "seizure," and the government conducts the subsequent "search." *Cf. Bach*, 310 F.3d at 1067-68. Preservation under § 2703(f) is the "seizure" part of the Stored Communications Act's

---

electronic copies of the defendant's personal computer "deprived him of exclusive control over those files," which was "a meaningful interference with [the defendant's] possessory rights in those files and constituted a seizure within the meaning of the Fourth Amendment."), *vacated by United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016) (*en banc*).

procedure for obtaining Internet account contents. Preservation does not cause a search to occur, because information is not yet revealed to the government. But the transfer of control of account contents under § 2703(f) is a seizure independently of any subsequent search, and it must be independently justified as reasonable. *See Soldal,* 506 U.S. at 61 (explaining that seizures must be justified under the Fourth Amendment independently of any searches).[4]

C. THE PROVIDERS' TERMS OF SERVICE DID NOT ELIMINATE MR. MEEK'S FOURTH AMENDMENT RIGHTS.

The violation of Mr. Meek's Fourth Amendment rights was not lessened or eliminated by the Terms of Service that apply to the Providers' accounts. Terms of Service found in contracts of adhesion between Internet providers and their users cannot control users' Fourth Amendment rights.

Some background is in order. Every Internet account is governed by Terms of Service, also known as Terms of Use. Terms of Service are contractual terms, drafted by lawyers for the provider, that govern when Internet users can sue the corporation that provides the service for the service that it provides. As a condition of using the service, every user must agree to the Terms. To ensure users cannot sue providers for complying with law enforcement requests, Terms often state that the provider retains the right to comply with those requests. *See, e.g.,* Meta Terms of Service, *available at* https://mobile.facebook.com/privacy/policy/version/20220104/ (reserving the right to "access, preserve and share your information with . . . law enforcement . . . [i]n response to a legal request").

---

[4] A small number of trial courts have reasoned that copying account contents are not seizures in the special context of copying files stored outside the United States. *See, e.g., United States v. Gorshkov*, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001) (copying from a server in Russia); *In re Search Warrant To Google, Inc.*, 2017 WL 2985391, at *11 (D.N.J. 2017) (copying accounts from servers outside the United States as part of the execution of a cloud warrant). This case does not raise the unique international concerns that underlay those decisions.

Whatever legal effect Terms of Service may have, they do not eliminate user Fourth Amendment rights or amount to consent. Terms of Service are private contracts between private Internet companies and private users such as the defendant. Although an access agreement between a private person and *the government* can create consent to a search or seizure, an access agreement between a private person and company such as Google, Apple, Snapchat or Dropbox cannot.

This point is clearly established by caselaw about rental car contracts and apartment leases. For example, in *Byrd v. United States*, 138 S.Ct. 1518 (2018), the Supreme Court held that being an unauthorized driver of a rental car in violation of the contract does not eliminate a reasonable expectation of privacy in the car. *See id.* at 1529 ("As anyone who has rented a car knows, car-rental agreements are filled with long lists of restrictions. . . .. Few would contend that violating provisions like these has anything to do with a driver's reasonable expectation of privacy in the rental car—as even the Government agrees.") Private contracts such as rental car agreements are about "risk allocation" between companies and customers, and they have "little to do with whether one would have a reasonable expectation of privacy" in the item used. *Id.*

The same is true with apartment leases. In *United States v. Washington*, 573 F.3d 279 (6th Cir. 2009), the government argued that the defendant had no reasonable expectation of privacy in an apartment because his presence violated the apartment's lease. The Sixth Circuit flatly rejected the claim because "the very premise of the government's argument is flawed." *Id.* at 284. Merely violating the contract could not eliminate privacy rights, the court reasoned, as such a rule would have "the intolerable implications" that a person's rights could be easily relinquished by a common contractual breach. *Id.* at 284. "[W]e reject the notion that the

Constitution ceases to apply in these circumstances." *Id.* at 285. *See also State v. Jacques*, 210 A.3d 533 (Conn. 2019) (citing other cases).

What was true for rental car contracts in *Byrd*, and apartment leases in *Washington*, is equally true for Terms of Service in this case. Terms of Service for Internet accounts are written by corporate lawyers to allocate corporate risk. Terms of Service ensure that a company cannot be sued for violating the service's privacy policy when taking steps the company is legally obligated to take or may want to take for legitimate business reasons. *See* Judith A. Powell & Lauren Sullins Ralls, *Best Practices for Internet Marketing and Advertising*, 29 Franchise L.J. 231, 235 (2010) (advising website operators on considerations for crafting Terms of Service). To limit corporate liability, Terms of Service are written to limit user permissions while granting providers broad rights. *See, e.g., United States v. Nosal*, 676 F.3d 854, 860–63 (9th Cir. 2012) (providing examples). Such form language designed to minimize corporate risk did not narrow or eliminate Fourth Amendment rights in *Byrd* or *Washington* and cannot do so here.

Finally, even if Terms of Service could eliminate Fourth Amendment rights in theory, they cannot do so in practice because the formal act of clicking on a box to agree to Terms of Service cannot be construed as granting consent under *Florida v. Jimeno*, 500 U.S. 248 (1991). *Jimeno* held that the scope of consent is determined by asking "what would the typical reasonable person have understood by the exchange" purporting to grant consent. *Id.* at 251. As applied to Internet accounts, the question is whether a reasonable person observing a user's formal agreement to Terms of Service would understand the user to have actually consented to its specific language.

The answer to that question is "no." A reasonable person would not understand the formality of agreeing to Terms of Service as signifying actual agreement to its terms for a simple

reason: Internet users almost never read Terms of Service. *See* Caroline Cakebread, *You're Not Alone, No One Reads Terms of Service Agreements*, Business Insider, November 17, 2017, https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 (discussing studies).

For example, in one study, academic researchers created a fake social media site called NameDrop. The Term of Use required "all users" of NameDrop "to immediately assign their first-born child to NameDrop, Inc." Jonathan A. Obar &Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, Information, Communication & Society 12 (2018).[5] Only about 2% of site users objected to the term, as 74% of users did not view the Terms of Service and most who viewed them scrolled through the legalese too quickly to understand them. *See id*. at 2.

Obviously, a "typical reasonable person" would not interpret a user's clicking on a box to express agreement with NameDrop's Terms of Service as actually consenting to give their first-born child away. *Jimeno*, 500 U.S. at 251. Rather, a reasonable person would interpret clicking on the box as just agreeing to use the site without concern for what the Terms say. *See* Obar & Oeldorf-Hirsch, *supra*. The same is true for Mr. Meek's act of clicking on the box to use the Providers Accounts. Whatever legal effect the Terms of Service may have in other contexts, clicking on a box to use the service cannot eliminate Mr. Meek's Fourth Amendment rights and does not establish consent.

---

[5] This paper is available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465.

D. THE ENTIRE CONTENTS OF THE PRESERVED ACCOUNTS MUST BE SUPPRESSED AS FRUITS OF THE POISONOUS TREE.

Circumstances indicate that preserved copies of several of Defendant's Accounts were turned over to the government. Because the government only had access to that preserved copy as a result of its prior constitutional violation, the entire contents of the account must be suppressed as fruits of the poisonous tree under *Wong Sun v. United States*, 371 U.S. 471 (1963).

Suppression is appropriate when, among other things, it "results in appreciable deterrence." *Herring v. United States*, 555 U.S. 135, 141 (2009). That is the case here. Suppression is needed to deter massive-scale and ongoing violations of the Fourth Amendment. Every year, hundreds of thousands of Internet accounts are preserved based on the baseless assumption that 18 U.S.C. § 2703(f) permits unlimited and suspicionless preservation. *See* Kerr, *Internet Content Preservation*, at 755. Preservation occurs almost entirely in secret, and therefore has gone unchallenged, because governments and Internet providers do not notify their users that preservation has occurred. *See id.* at 771, 775-78. Preservation has occurred on a massive scale nationwide because it has been treated—wrongly, and in the absence of caselaw—as a constitution-free process.

Suppression of the evidence in this case would have a powerful effect "in deterring Fourth Amendment violations in the future." *Herring*, 555 U.S. at 141. A single court ruling could alter practices nationwide. At present, "preservation under § 2703(f) occurs on a wide scale with little scrutiny because law enforcement and providers consider it a privacy non-event." Kerr, *Internet Content Preservation*, at 756. Many if not most preservations that occur today likely violate the Fourth Amendment. A decision from this court suppressing the evidence would be read and digested by both government lawyers nationwide and lawyers at the major Internet providers. A suppression order in this case would force the government to bring its preservation

practices within constitutional bounds. It would both limit when investigators seek preservation and trigger provider scrutiny of preservation requests.

A suppression order would have an indirect effect, as well. By identifying constitutional limits on preservation, this court's ruling would encourage providers to disclose preservation to their users, and force governments to disclose preservation to defendants, so that other individuals could more readily litigate potential violations of their Fourth Amendment rights. It is rare that a single court ruling could have such a nationwide impact. But this is such a case. Under Supreme Court precedent, that deterrent effect justifies suppression. *See Herring*, 555 U.S. at 700.

Finally, the good-faith exception of *Illinois v. Krull*, 480 U.S. 340 (1987), poses no barrier to suppression. *Krull* held that the exclusionary rule does not apply "when officers act in objectively reasonable reliance upon a statute authorizing warrantless administrative searches, but where the statute is ultimately found to violate the Fourth Amendment." *Id.* at 342. Officers are entitled to rely on legislative judgments that searches are constitutional, *Krull* reasoned, at least when those legislative judgments are reasonable. *See id.* at 349-50.

Krull does not apply because the mistake here belongs to law enforcement instead of Congress. When Congress enacted 18 U.S.C. § 2703(f), it did not make any legislative judgments about what law enforcement seizures are permitted or when they are constitutional. The preservation statute is not directed to governments at all. The Fourth Amendment governs when a preservation request can be made, and the preservation statute does not say otherwise. The preservation statute merely specifies what Internet providers, such as those here, must do when a government preservation request is made. "[U]pon the request of a governmental entity,"

the statute says, "[a] provider . . . shall take all necessary steps to preserve records and other evidence in its possession" 18 U.S.C. § 2703(f)(1).

It may be that investigators erroneously believed that § 2703(f) authorizes unlimited preservation. But, if so, that is a law enforcement mistake that falls outside *Krull*. Because there is no legislative error to defer to, the government cannot rely on *Krull* to avoid suppression. *See United States v. Wallace,* 885 F.3d 806, 811 n.3 (5th Cir. 2018) (noting, in a Fourth Amendment challenge brought to surveillance claimed to be authorized by the Stored Communications Act, that "[t]he holding of *Krull* does not extend to scenarios in which an officer erroneously, but in good faith, believes he is acting within the scope of a statute"); *People v. Madison*, 520 N.E.2d 374, 380 (Ill. 1988) (ruling that *Krull* cannot apply where a "police officer reasonably relies on his own interpretation of a valid statute in conducting a search and seizure" but courts later reject that interpretation).

Put another way, *Krull* only applies when a legislature enacts an unconstitutional law that law enforcement reasonably followed. Here, however, Congress enacted a perfectly constitutional law. Law enforcement's unconstitutional application of the preservation statute is law enforcement's fault, not the fault of Congress. The exclusionary rule should apply.

CONCLUSION

For the foregoing reasons, the Mr. Meek respectfully requests that this court suppress all evidence obtained as a result of the unlawful seizure of Mr. Meek's Accounts. In the alternative, this Court should order an evidentiary hearing to determine whether to grant this Motion to Suppress.

Respectfully Submitted,

By: /s/ *Eugene V. Gorokhov*
Eugene Gorokhov, Bar No. 73582
Attorney for Defendant
BURNHAM & GOROKHOV, PLLC
1750 K Street NW, Suite 300
Washington, DC 20006
(202) 386-6920 (phone)
(202) 765-2173 (fax)
eugene@burnhamgorokhov.com

CERTIFICATE OF SERVICE

I hereby certify that I filed the foregoing document VIA ECF which provides a copy to the AUSA of record.

By: /s/ *Eugene V. Gorokhov*
Eugene Gorokhov, Bar. No. 73582
Attorney for Defendant
BURNHAM & GOROKHOV, PLLC
1750 K Street NW, Suite 300
Washington, DC 20006
(202) 386-6920 (phone)
(202) 765-2173 (fax)
eugene@burnhamgorokhov.com